



MEDIDAS Y RECOMENDACIONES
DE SEGURIDAD DE LA INFORMACIÓN
Y CIBERSEGURIDAD PARA
VENTA NO PRESENTE



Realiza tus compras únicamente en sitios WEB de confianza.



Revisa que los sitios o páginas WEB en donde realizas tus compras inicien con las letras <https://> y que tengan un ícono de un candado cerrado, es decir, un certificado de confianza.



Verifica muy bien las condiciones del pago antes de realizarlo, como lo es el valor, número de cuotas, periodicidad del pago, renovaciones automáticas, entre otras.



Los pagos electrónicos debes realizarlos desde redes seguras, evita realizarlos en redes abiertas o inseguras como los cafés Internet. En lo posible, utiliza redes privadas virtuales (VPN) para incrementar la seguridad del pago.



Realiza tus pagos desde equipos o dispositivos confiables.



El equipo o dispositivo desde el cual realizas el pago debe tener todas las actualizaciones de seguridad y contar con software antivirus instalado y actualizado.



Verifica que el equipo o dispositivo desde el cual realizas el pago no tenga instaladas aplicaciones sospechosas o desconocidas, estas podrían poner en riesgos la información.



Si vas a descargar aplicaciones móviles, asegúrate de hacerlo directamente de las tiendas oficiales como Google Play o Apple Store.



Crea un patrón o PIN seguro de acceso a tus teléfonos inteligentes y tabletas.



No utilices fechas de cumpleaños o números consecutivos, nombres de familiares y mascotas.



Utiliza contraseñas seguras, es decir compuestas por al menos 8 caracteres entre letras, números, mayúsculas, minúsculas y símbolos (por ejemplo # \$ % & + *).



Limita los montos de los pagos, esto evitará que un eventual fraude tenga mayor impacto.



No accedas a las tiendas o comercios por enlaces que te lleguen al correo electrónico, para mayor seguridad digita la dirección directamente en el navegador.



Desconfía de promociones u ofertas extremadamente atractivas, confirma con el comercio la validez de esta.



Ante dudas o sospechas de situaciones anormales, comunícate inmediatamente con tu Banco. No escribas ni almacenes el código de validación (CVV2) en ningún lado, debes memorizarlo para una mayor seguridad.